D-Link®
Building Networks for People

Manual

Version 1.0

DGL-4300

Wireless 108G Gaming Router

Contents

Package Contents 6
Minimum System Requirements 6
Introduction 7
Features and Benefits 8
Hardware Overview 9
Connections 9
LEDs 10
Wireless Basics 11
Standards-based Technology 12
Installation Considerations 12
Using the Configuration Interface 13
Basic 13
Wizard 13
Internet Connection Setup Wizard 14
Wireless Security Setup Wizard 16
WAN 18
Modes 18
Advanced 19
Static WAN Mode 20
DHCP WAN Mode 20
PPPoE WAN Mode 21
LAN 21
LAN Settings 21
DHCP 22
DHCP Settings 22
Number of Dynamic DHCP Clients 22
Add Static DHCP Client 23
Static DHCP Client List 23

Wireless *24*
Basic Wireless Settings 24
Wireless Security Mode *25*
WEP 25
WPA-Personal 26
WPA-Enterprise 26
Advanced 27
Virtual Server *27*
Add/Edit Virtual Server 28
Virtual Servers List 28
Special Applications *29*
Application Level Gateway (ALG) Configurations 29
Add/Edit Special Applications Rule *30*
Special Applications Rules List *30*
Gaming *31*
Add/Edit Game Rule 31
Game Rules List 31
GameFuel™ *32*
GameFuel™ Setup 32
Add/Edit GameFuel™ Rule 33
GameFuel Rules List 33
Routing *34*
Add/Edit Route 34
Route List 34
Access Control *35*
Enabled 35
Add/Edit Access Control Rule 35
Access Control Rules List 36
Web Filter *36*
Add/Edit Web Site 36
Allowed Web Site List 36

Mac Address Filters *37*
Filter Settings 37
Add MAC Address 37
MAC Address List 37
Firewall *38*
Firewall Settings 38
Inbound Filters *39*
Add/Edit Inbound Filter Rule 39
Inbound Filter Rules List 39
Configuring an Inbound Filter Rule 40
Advanced Wireless *41*
Advanced Wireless Settings 41
Tools 42
Admin *42*
Password 42
Administration 42
Save and Restore Configuration 42
Time *43*
Time Configuration 43
Set the Date and Time 43
Schedules *44*
Add/Edit Schedule Rule 44
Schedule Rules List 44
Syslog *45*
Email *45*
Email Settings 45
Email Log When Full or on Schedule 45
System *46*
System Commands 46
Firmware *47*
Firmware Information 47

Firmware Upgrade 47
Firmware Upgrade Notification Options 47
Dynamic DNS 48
Status 49
Device Info 49
General 49
WAN 49
LAN 49
Wireless LAN 50
Wireless 50
Routing 50
Logs 51
Log Options 51
Log Details 51
Statistics 51
Network Traffic Stats 51
LAN Statistics 52
WAN Statistics 52
Wireless Statistics 52
Active Sessions 52
Appendix 53
Securing Your Network 53
Glossary 55
Technical Specifications 65
Contacting Technical Support 67
Warranty 68
Registration 72

Package Contents

- D-Link® DGL-4300 GamerLounge™ Gaming Router
- Detachable Antenna
- Cat5 Ethernet Cable
- Power Adapter (5.0V, 2.5A)
- CD-ROM with Manual
- Quick Installation Guide
- Vertical Stands
- Rubber Feet

Note: Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.

If any of the above items are missing, please contact your reseller.

Minimum System Requirements

- Ethernet-Based Cable or DSL Modem

To Change Default Settings

- PC with
- 1.2GHz Processor
- 256MB Memory
- CD-ROM Drive
- Ethernet Adapter with TCP/IP Protocol Installed
- Windows® XP/2000/Me or Mac® OS X v10.3/v10.2/v10.1
- Internet Explorer v6 or Netscape® Navigator v7

Introduction

The D-Link GamerLounge™ DGL-4300 High-Speed Wireless Gaming Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking and is designed to provide maximum gaming performance.

With top-notch maximum wireless signal rates of up to 108Mbps[1] and Gigabit Ethernet support for 10/100/1000Mbps LAN connections, rest assured enough bandwidth is available for all your gaming needs.

The DGL-4300 incorporates GameFuel™ Technology designed to provide the uninterrupted and flawless gaming experience serious online gamers expect.

The DGL-4300's high-performance CPU supports up to 1000 concurrent connections, making it ideal for P2P applications and multiplayer interactivity.

[1]Maximum wireless signal rate derived from IEEE Standard 802.11a/11b/11g specifications. Actual data throughput will vary. Network conditions and environmental factors lower actual data throughput rate.

Features and Benefits

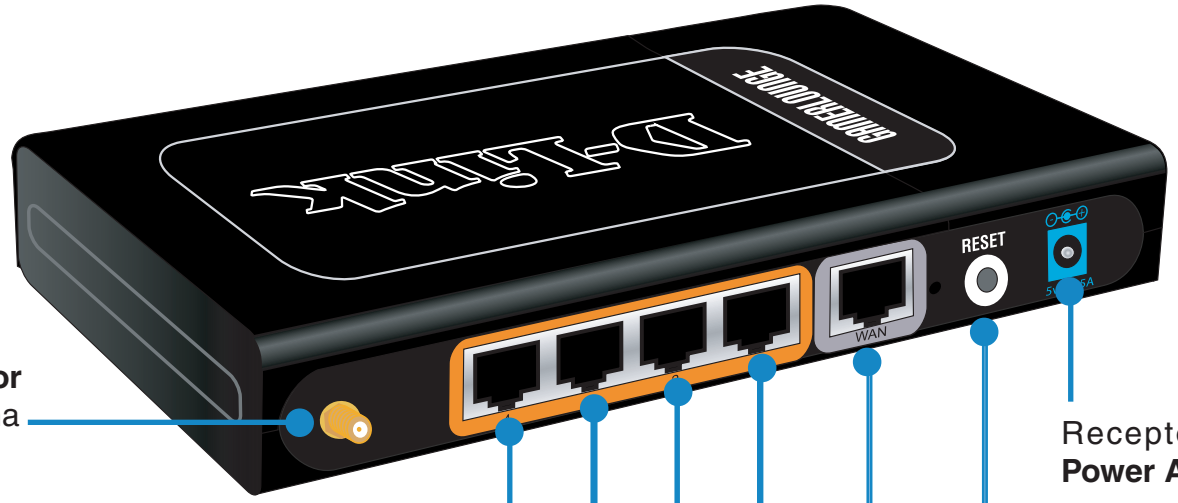
- Loaded with game-centric features boasting maximum flexibility for configuration and performance
- Designed for the Gamers Network
- GameFuel Priority powered platform delivers fully-loaded features boosting network efficiency and performance
- Enhanced wireless technology for optimal range and connectivity – up to 108Mbps[1]
- High-Performance CPU – ideal for P2P applications and multiplayer interactivity
- Automatically prioritizes and intelligently manages network traffic to better execute bandwidth-sensitive applications such as VoIP and multimedia streaming
- Enables multi-tasking between other applications without degradation in game connection
- Pre-configured ports to accommodate up to 256 policies for games and applications
- Customizable settings to add or modify new applications or game configurations
- New firmware upgrade notification keeps your D-Link Gaming Router up-to-date
- Next Generation hardware with one Fast Ethernet 10/100 WAN port and four Gigabit Ethernet 10/100/1000 auto-sensing LAN ports
- Shamelessly attractive chassis – chrome-plated front panel, hypnotizing blue LEDs
- 5dBi high-gain antenna for exceptional wireless signal
- Smooth GUI design for seamless device management
- Protect your wireless data with both Wi-Fi Protected Access (WPA) and 128-bit Wired Equivalent Privacy (WEP)
- Integrated Stateful Packet Inspection (SPI) firewall and Network Address Translation (NAT) firewall help protect against hackers, wardrivers, and other unauthorized users
- Create versatile Access Control policies to control network access based on time, date, websites, and/or applications
- Disable SSID Broadcast and MAC Filtering features help increase your level security to protect against unauthorized access to your wireless network
- Supports Virtual Private Network (VPN) pass-through to create a secure connection to your day job

[1]Maximum wireless signal rate derived from IEEE Standard 802.11a/11b/11g specifications. Actual data throughput will vary. Network conditions and environmental factors lower actual data throughput rate.

Hardware Overview

Connections

All Ethernet Ports (WAN and LAN) are auto MDI/MDIX, meaning you can use either a straight-through or a crossover Ethernet cable.



Antenna Connector
for wireless antenna

Auto MDI/MDIX LAN ports automatically sense the cable type when connecting to Ethernet-enabled computers.

The **Auto MDI/MDIX WAN** port is the connection for the Ethernet cable to the Cable or DSL modem.

Pressing the **Reset Button** restores the router to its original factory default settings.

Receptor for the **Power Adapter**

LEDs

LOCAL NETWORK LEDs
A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission

WLAN LED
This LED will blink to indicate activity on the wireless network

POWER LED
A solid light indicates a proper connection to the power supply

WAN LED
A solid light indicates connection on the WAN port. This LED blinks during data transmission

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business, or on public access wireless networks. D-Link wireless products will allow you access to the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking brings.

A WLAN is a cellular computer network that transmits and receives data with radio signals instead of wires. WLANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

People use wireless LAN technology for many different purposes:

Mobility - Productivity increases when people have access to data in any location within the operating range of the WLAN. Management decisions based on real-time information can significantly improve worker efficiency.

Low Implementation Costs – WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLANs ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation and Network Expansion - Installing a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Wireless technology allows the network to go where wires cannot go - even outside the home or office.

Scalability – WLANs can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to larger infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Inexpensive Solution - Wireless network devices are as competitively priced as conventional Ethernet network devices.

Standards-based Technology

The DGL-4300 Wireless Broadband Router utilizes the new **802.11g** standard.

The IEEE **802.11g** standard is an extension of the 802.11b standard. It increases the data rate up to 54Mbps within the 2.4GHz band, utilizing **OFDM technology**.

This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing **OFDM** (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) technology. **OFDM** works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. **OFDM** reduces the amount of **crosstalk** (interference) in signal transmissions.

The DGL-4300 is backwards compatible with 802.11b devices. This means that if you have an existing 802.11b network, the devices in that network will be compatible with 802.11g devices at speeds of up to 11Mbps in the 2.4GHz range.

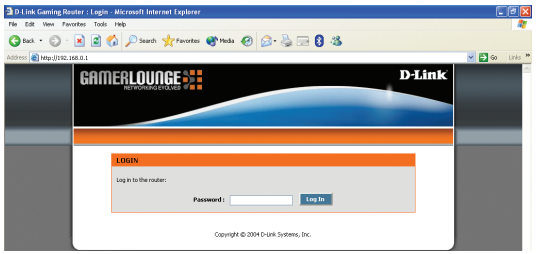
Installation Considerations

The D-Link DGL-4300 lets you access your network, using a wireless connection, from virtually anywhere within its operating range. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

- Keep the number of walls and ceilings between the DGL-4300 and other network devices to a minimum - each wall or ceiling can reduce your D-Link wireless product's range from 3-90 feet (1-30 meters). Position your devices so that the number of walls or ceilings is minimized.
- Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.
- Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.
- Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate extreme RF noise.

Using the Configuration Interface

The Configuration Interface can be accessed from your Web browser. Open up your Web browser and type **http://192.168.0.1** in the address field and press **Enter**. The Configuration Interface login screen will appear. By default, there is no password. Click on the **Log In** button to access the Configuration main screen.



Basic

The Basic settings tab contains the Setup Wizards, Internet connection, and network setting options.

Wizard

The Wizard screen contains two wizards that assist you with the configuration of your D-Link® Gaming Router.

Basic > Wizard

Internet Connection Setup Wizard

The Internet Connection Setup Wizard will assist you with connecting your D-Link® Gaming Router to the Internet. The step by step guide will prompt you for the necessary information to get you connected. The Internet Connection Setup Wizard guides you through the following basic router setup steps:

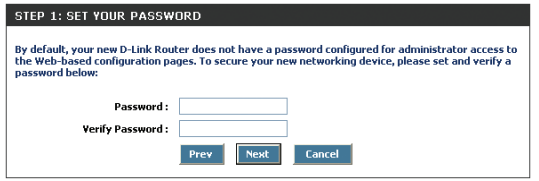
To begin, click on the **Launch Internet Connection Setup Wizard** button.

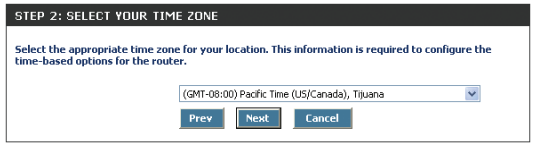
- The **Welcome To The D-Link Setup Wizard** screen appears, click Next to continue.

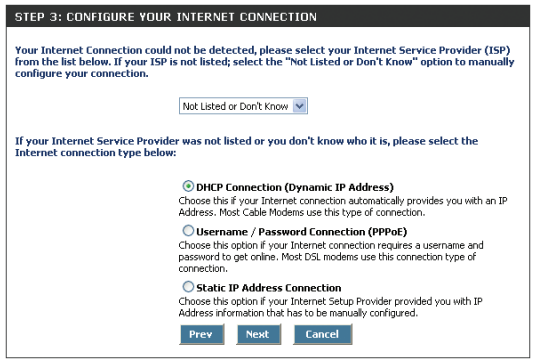
- **Step 1: Set Your Password** prompts you to enter a password for the Web-based configuration interface. You must also enter the password in the Verify Password prompt.

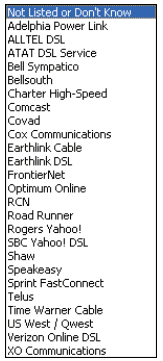
- **Step 2: Select Your Time Zone** prompts you to select your time zone from the pull-down menu.

- **Step 3: Configure Your Internet Connection** prompts you to select your Internet Service Provider from the pull-down menu. If your Internet Service Provider is not listed or you do not know who it is, you can select the connection type manually.



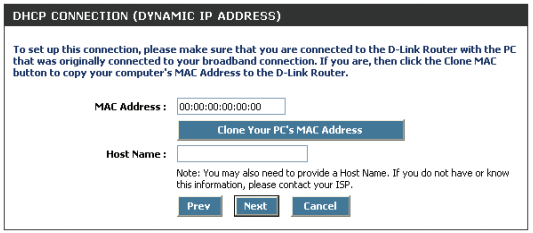




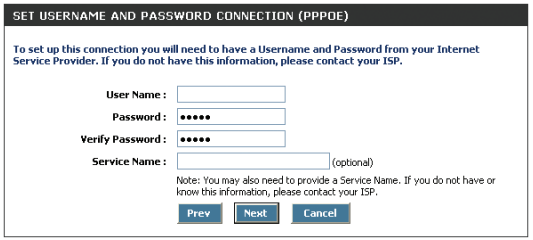


Depending upon your Internet Service Provider or the type of connection you selected in the previous step, one of three screens will appear. If you are unsure of any of the information, please contact your Internet Service Provider (ISP) for details.

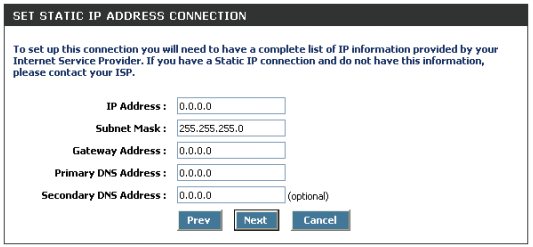
- **DHCP Connection (Dynamic IP Address)** requires you to enter the MAC address of the computer that was originally connected to your broadband modem. If you are using that computer, click on the **Clone Your PC's MAC Address** button and the MAC address is automatically copied. If your ISP requires you to enter a Host Name, please do so.



- **Set Username and Password Connection (PPPoE)** prompts you to enter your Username and Password. You must also verify the Password. If your ISP requires a Service Name entry, please enter it here.



- **Set Static IP Address Connection** prompts you to enter the IP address, Subnet Mask, Gateway Address, Primary and Secondary DNS address information.



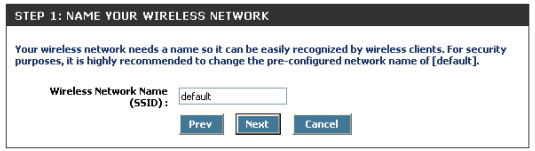
- **Setup Complete** will appear after all of the settings have been entered. Click **Connect** to save your settings and reboot the router.

Wireless Security Setup Wizard

The Wireless Security Setup Wizard will assist you with setting up your wireless network. The step by step guide will ask you for the necessary information to secure your wireless network. The Wireless Security Setup Wizard guides you through the following steps:

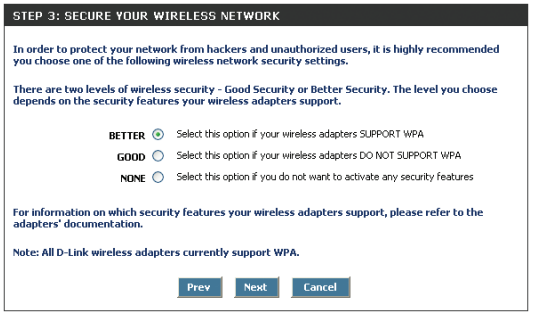
To begin, click on the **Launch Wireless Security Setup Wizard** button.

- The **Welcome To The D-Link Wireless Security Setup Wizard** screen appears, click Next to continue.



- **Step 1: Name Your Wireless Network** prompts you to enter a wireless network name for your network. This name is also referred to as SSID. For security purposes, it is highly recommended that you do not use the default name.

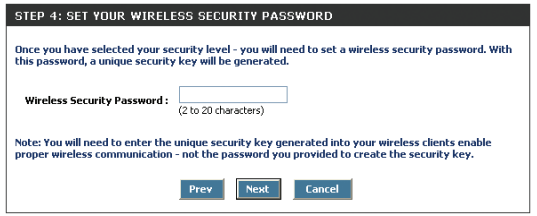
- **Step 2: Select A Channel for your Wireless Network** prompts you to select the channel that will be used by your router to communicate to wireless devices.



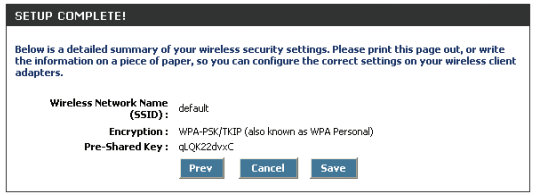
- **Step 3: Secure Your Wireless Network** prompts you to select the level of security that you want to use on your wireless network.

Depending upon your selection in Step 3, you will see one of the following screens.

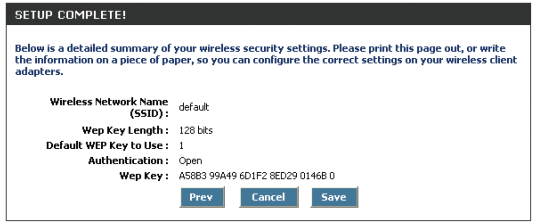
- **Step 4: Set Your Wireless Security Password** prompts you to enter a wireless security password between 2 and 20 characters in length.



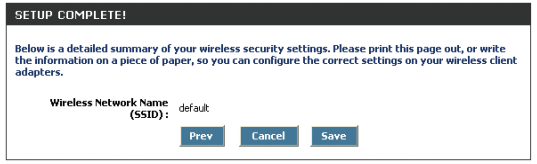
- If you selected **Better** security in step 3, this screen will appear providing you your pre-shared key information.



- If you selected **Good** security in step 3, this screen will appear providing you your WEP key information.



- If you selected **None** security in step 3, this screen will appear providing you your wireless network name.



WAN

The WAN section is where your Internet Connection mode is selected. Your Internet Service Provider (ISP) determines the type of connection that you use.

Modes

There are three connection modes to choose from as shown below. If you are unsure of your connection settings, contact your Internet Service Provider (ISP) and you can enter the necessary information on the QIG or print this page and write the settings for future reference.

Primary DNS Server: _____._____._____._____

Secondary DNS Server: _____._____._____._____

- **Static**: Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings.

  IP Address: _____._____._____._____

  Subnet Mask: _____._____._____._____

  Default Gateway: _____._____._____._____

- **DHCP**: A method of connection where the ISP assigns your IP address when your computer requests one from the ISP's server. Some ISP's require you to make some settings on your side before your computer can connect to the Internet.

  Host Name:_____

- **PPPoE**: A method of connection that requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

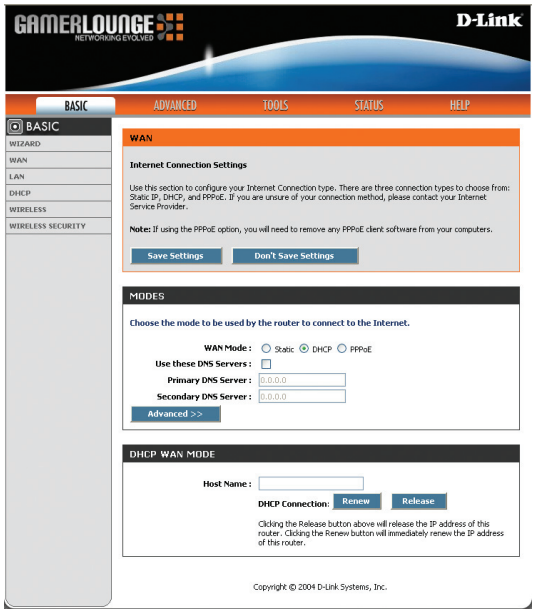
  Username:_____

  Password:_____

  Service Name (Optional):_____

All three modes have some common configuration options. The Primary and Secondary DNS Server settings are required for Static configurations and optional for DHCP and PPPoE configurations. The Advanced options on the following page can be modified for any of the three connection modes.

You should be able to get the **Primary DNS and Secondary DNS Servers** settings from your router configuration settings, ISP, or your network administrator. Only the primary DNS server address is required, though it is best to have both the primary and secondary addresses.



Basic > WAN

Advanced

The Advanced options apply to all WAN modes.

MTU: The MTU (Maximum Transmission Unit) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

Use the Default MTU: This option is enabled by default allowing the router to select the typical MTU settings for the selected WAN interface. If this option is unchecked, the router will use the value assigned in the MTU field.

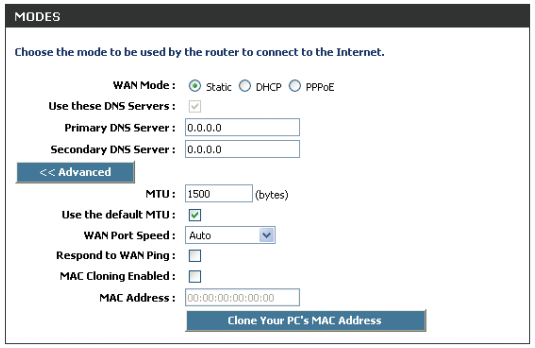
WAN Port Speed: The WAN Port Speed is set to auto by default. If you have trouble connecting the WAN port, you can select the connection type (10 or 100Mbps).

Respond to WAN Ping: This option is disabled by default. By disabling the WAN ping, the router will not respond to requests from a ping command received via the Internet. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

MAC Cloning Enabled: Some ISP's may check your computer's MAC address. Each networking device has it's own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer with this particular MAC address. The D-Link router has a different MAC address than the computer that initially connected to the ISP. To resolve this problem, enable this option.

MAC Address: When MAC Cloning is enabled, you can enter in a MAC address manually in this field or click the Clone Your Computer's MAC Address button.

Clone Your PC's MAC Address: When this button is clicked, the WAN port will use the MAC Address of the network adapter in the computer that you are using to access the router.



Basic > WAN > Advanced

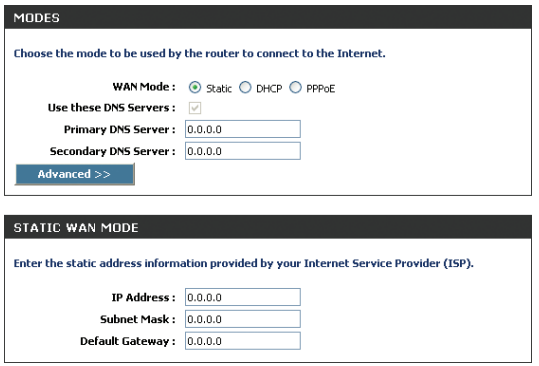
Static WAN Mode

Used when your ISP provides you a set IP address that does not change. The IP information is manually entered in your IP configuration settings.

IP Address: Input the IP Address provided from your router configuration settings, ISP or network administrator.

Subnet Mask: Input the Subnet mask provided from your router configuration settings, ISP or network administrator.

Default Gateway: Input the Gateway address provided from your router configuration settings, ISP or network administrator.



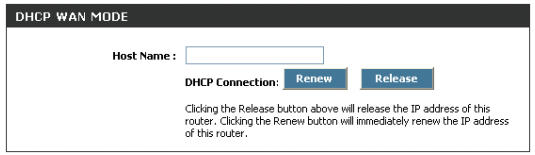
Basic > WAN > Static

DHCP WAN Mode

A method of connection where the ISP assigns your IP address when your computer requests one from the ISP's server. Some ISP's require you to make some settings on your side before your computer can connect to the Internet.

Host Name: Some ISP's may check your computer's HOST name. The HOST name identifies your system to the ISP's server. This way they know your computer is eligible to receive an IP address. In other words, they know that you are paying for their service.

DHCP Connection: The **Release** button will release the current IP address of the router. The **Renew** button will request an IP address.



Basic > WAN > DHCP

PPPoE WAN Mode

A method of connection that requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

Username: The username that you use to login to your Internet connection.

Password: Enter the password associated with your username.

Verify Password: Retype the password for verification.

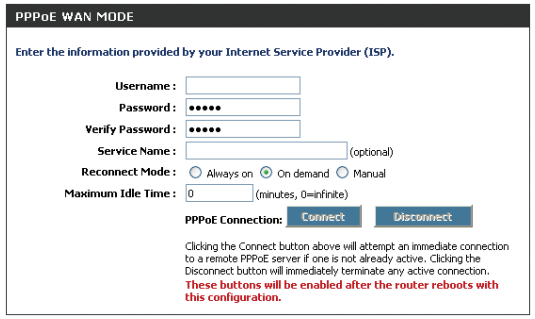
Service Name: If your ISP requires a service name, enter it here.

Reconnect Mode: Typically PPPoE connections are not always on. The D-Link Router allows you to set the connection mode:

- **Always on**: A connection to the Internet is always maintained.
- **On demand**: A connection to the Internet is made as needed.
- **Connect Manually**: You have to open up the Web-based management interface and click the Connect button manually any time that you wish to connect to the Internet.

Maximum Idle Time: Defines how long the machine can be idle before the PPPoE connection is disconnected.

PPPoE Connection: The **Disconnect** button will immediately terminate any active connection. *Note: These buttons become enabled after the router has been rebooted with the PPPoE mode selected.*



Basic > WAN > PPPoE

LAN

Your internal network settings are configured based on the IP Address and Subnet Mask assigned in this section. The IP address is also used to access this Web-based management interface. It is recommended that you use the default settings if you do not have an existing network.

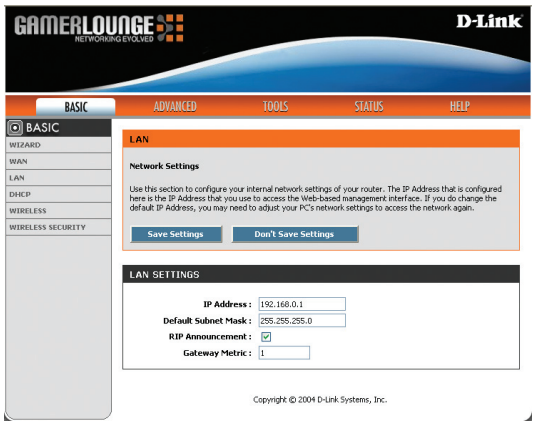
LAN Settings

IP Address: The IP address of the router on the local area network. The local network settings are based on the address assigned here.

Default Subnet Mask: The subnet mask of your router on the local area network.

RIP Announcement: Used with multiple routers to broadcast routing information.

Gateway Metric: This option is used if you have multiple routers.



Basic > LAN

DHCP

The DHCP section is where you configure the built-in DHCP Server to assign IP addresses to the computers and other devices on your local area network.

DHCP Settings

DHCP Server Enabled:

Once your D-Link Router is properly configured and this option is enabled, the DHCP Server function will assign your network devices the necessary information to connect to the LAN and Internet. This eliminates the need to manually configure each device on your network with IP settings.

Note: The devices on your network must have TCP/IP bound to the Ethernet connection with the "DHCP" or "Obtain an IP address automatically" option enabled.

DHCP IP Address Range:

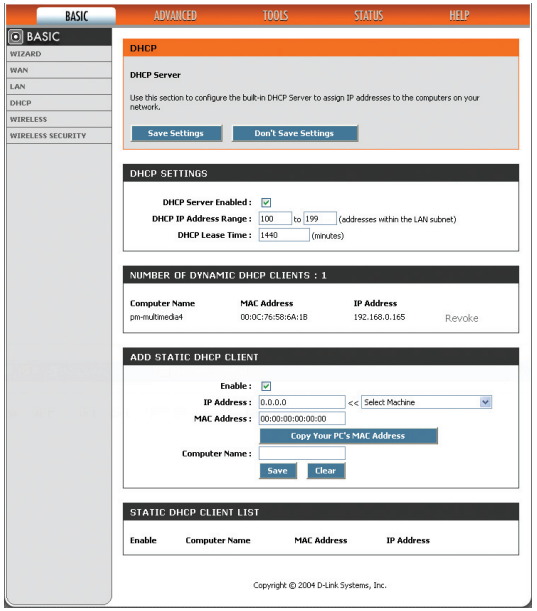
This option defines the range of addresses available for the Router to assign to your internal network. If you have any devices using static IP addresses, be sure the addresses do not fall within the range defined here. A Static IP address is one that is entered in manually on the device.

Example:

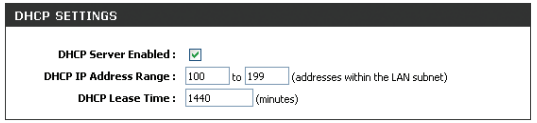
Your D-Link Router uses an IP address of 192.168.0.1. You've assigned a computer designated as a Web server with a static IP address of 192.168.0.2. You've assigned another computer designated as an FTP server with a static IP address of 192.168.0.3. The starting IP address for your DHCP server needs to be 192.168.0.4 or above.

DHCP Lease Time:

The amount of time a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease expires then a new lease is established. If the lease expires and the address is no longer needed, then another tenant may use the address.

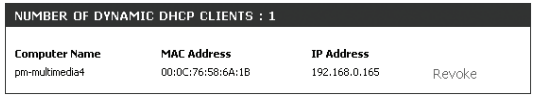


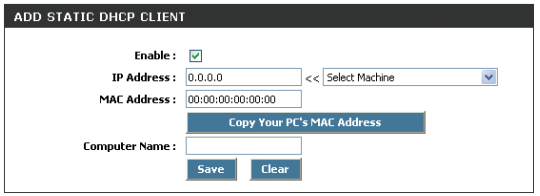
Basic > DHCP



Number of Dynamic DHCP Clients

In this section, you can see what LAN devices are currently leasing IP addresses. The DHCP Client table displays the number of clients that are receiving an IP address from the router. The computer name, MAC address, and IP address assigned to each computer are displayed here as well. You can **Revoke** IP addresses in this section. The **revoke** option allows you to tale away a leased IP address from a client. This feature is useful for freeing up addresses when the client table is full or nearly full. Be sure to only revoke addresses from devices that are no longer needed on the network.





Add Static DHCP Client

Static DHCP Clients receive the same IP address all the time. This is almost the same as if a device has a static IP address except that it must still actually request an IP address from the D-Link Router. The D-Link Router will provide the device the same IP address all the time. Servers on your network should either use a static IP address or this option. To input the MAC address of your system, enter it in manually or connect to the D-Link Router's Web-Management interface from the system and click the Copy Your PC's MAC Address button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the D-Link Router from the computer and use the **Copy Your PC's MAC Address** option to enter the MAC address.

Example: You have an FTP server that you want to share files over the Internet. You can connect to the D-Link Router from the computer designated as the FTP server.

1. Enter a designated IP address somewhere between the Starting IP and Ending IP addresses.
2. Click the **Copy Your PC's MAC Address** button and the D-Link Router will detect the MAC address and enter it automatically.
3. The computer name can be entered in for reference but is not required.
4. Click the OK button and then click on the Save Settings button at the top of the page.

The IP address will now only be assigned to the designated computer and it will always receive the same IP address as long as it uses the same Ethernet adapter.

Note: If you replace the Ethernet adapter in a computer that is using Static DHCP, you will need to Copy the PC's MAC Address again because every Ethernet adapter has a unique MAC address. The same goes for any network device. If you replace a network device such as a print server, you will need to input the MAC address of the new print server into the Static DHCP configuration.

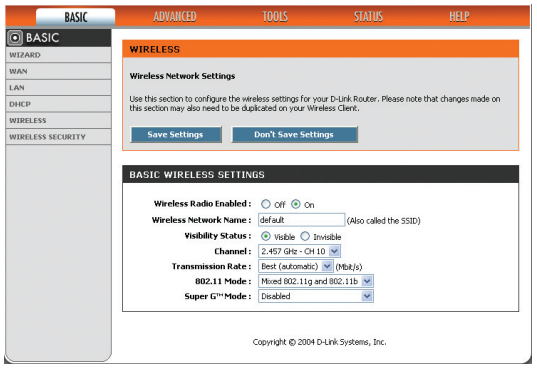
Static DHCP Client List

Entries on this list can be enabled/disabled by toggling the Enable checkbox. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Wireless

The wireless section is used to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

Basic Wireless Settings



Basic > Wireless

Wireless Radio Enabled: This option turns off and on the wireless connection feature of the router. If this is not enabled, you cannot connect using a wireless network adapter.

Wireless Network Name: When you are browsing for available wireless networks, this is the name that will appear in the list (unless Visibility Status is set to Invisible, see below). This name is also referred to as the SSID.

Visibility Status: The Invisible option allows you to hide your wireless network. When this option is set to Visible, your wireless network name is broadcast to anyone within the range of your signal. If you're not using encryption then they could connect to your network. When Invisible mode is enabled, you must enter the Wireless Network Name (SSID) manually to connect to the network.

Channel: Select the channel with the clearest signal.

Transmission Rate: By default the transmission rate will automatically select the fastest rate. You have the option of selecting the speed if necessary.

802.11 Mode: If all of your devices can connect in 802.11g Mode then leave the setting at 802.11g only. If you have some devices that are 802.11b than you can change the mode to Mixed.

Super G™ Mode: Super G Turbo Modes must use channel 6 for transmission and 802.11 Mode must be set to 802.11g.

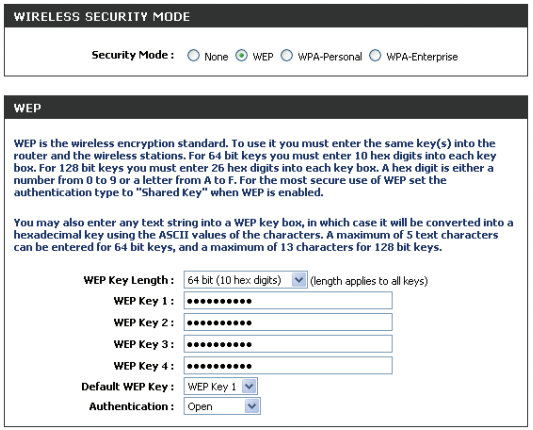
- **Super G without Turbo**: Performance enhancing features such as Packet Bursting, FastFrames, and Compression.
- **Super G with Static Turbo**: Mode is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all devices on the wireless network are Super G with Static Turbo enabled.
- **Super G with Dynamic Turbo**: Mode is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all devices on the wireless network are Super G with Dynamic Turbo enabled.

Wireless Security Mode

To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

WEP

A method of encrypting data for wireless communication intended to provide the same level of privacy as a wired network. WEP is not as secure as WPA encryption. To gain access to a WEP network, you must know the key. The key is a string of characters that you create. When using WEP, you must determine the level of encryption. The type of encryption determines the key length. 128-bit encryption requires a longer key than 64-bit encryption. Keys are defined by entering in a string in HEX (hexadecimal - using characters 0-9, A-F) or ASCII (American Standard Code for Information Interchange – alphanumeric characters) format. ASCII format is provided so you can enter a string that is easier to remember. The ASCII string is converted to HEX for use over the network. Four keys can be defined so that you can change keys easily. A default key is selected for use on the network.



Example:

64-bit hexadecimal keys are exactly 10 characters in length.
(12345678FA is a valid string of 10 characters for 64-bit encryption)

128-bit hexadecimal keys are exactly 26 characters in length.
(456FBCDF123400122225271730 is a valid string of 26 characters for 128-bit encryption)

64-bit ASCII keys are exactly 5 characters in length
(DMODE is a valid string of 5 characters for 64-bit encryption)

128-bit ASCII keys are exactly 13 characters in length
(2002HALOSWIN1 is a valid string of 13 characters for 128-bit encryption)

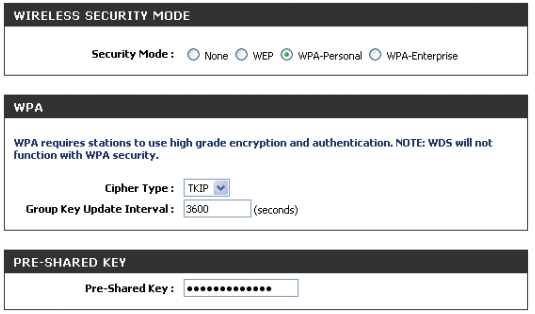
WPA-Personal

This option uses Wi-Fi Protected Access with a Pre-Shared Key (PSK).

Pre-Shared Key: The key is entered as a pass-phrase of up to 63 characters in ASCII format at both ends of the wireless connection. The pass-phrase cannot be shorter than 8 characters. The pass-phrase is used to generate session keys that are unique for each wireless client.

Cipher Type: The encryption algorithm used to secure the data communication. TKIP (Temporal Key Integrity Protocol) provides per packet key generation and is based on WEP. AES (Advanced Encryption Standard) is a very secure block based encryption.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.



WPA-Enterprise

This option works with a RADIUS server to authenticate wireless clients. Wireless clients should have established the necessary credentials before attempting to authenticate to the Server through the Gateway. Furthermore, the RADIUS Server may need to be configured to allow this Gateway to authenticate users.

Cipher Type: The method in which the pre-shared key is changed.

Group Key Update Interval: The amount of time before the group key used for broadcast and multicast data is changed.

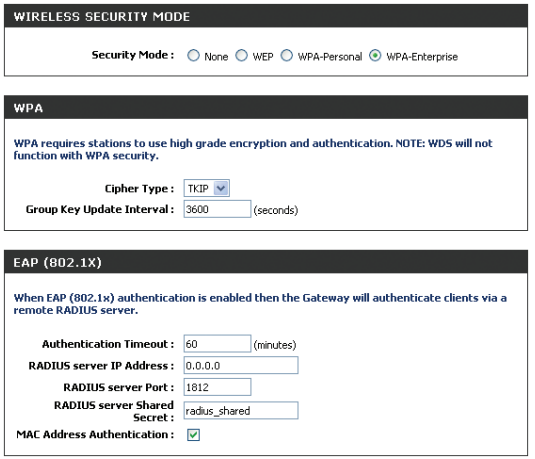
Authentication Timeout: Amount of time before a client is required to re-authenticate.

RADIUS Server IP Address: The IP address of the authentication server.

RADIUS Server Port: The port number used to connect to the authentication server.

RADIUS Server Shared Secret: A passphrase that must much with the authentication server.

MAC Address Authentication: If this is selected then the user will need to connect from the same computer whenever logging into the wireless network.



Advanced

The Advanced options allow you to configure a variety of advanced features including ports, application priority, Internet access, filters, and advanced wireless settings.

Virtual Server

The Virtual Server option gives Internet users access to services on your LAN. This feature is useful for hosting online services such as FTP, Web, or Game Servers. For each Virtual Server, you define a public port on your router for redirection to an internal LAN IP Address and port.

Example: You are hosting a Web Server on a PC that has Private IP Address of 192.168.0.50 and your ISP is blocking Port 80.

1. Name the Virtual Server Rule (ex. Web Server)
2. Enter in the IP Address of the machine on your LAN – 192.168.0.50
3. Enter the Private Port as [80]
4. Enter the Public Port as [8888]
5. Select the Protocol - TCP
6. Ensure the schedule is set to Always
7. Check the Add Rule to add the settings to the Virtual Server List
8. Repeat these steps for each Virtual Server Rule you wish to add. After the list is complete, click Save Settings at the top of the page.

With this Virtual Server Rule all Internet traffic on Port 8888 will be redirected to your internal web server on port 80 at IP Address 192.168.0.50.

Advanced > Virtual Server

Add/Edit Virtual Server

Virtual Server Rule:	Name of the virtual server, such as Web Server.
IP Address:	The IP address of the system on your internal network that will provide the virtual service, such as 192.168.0.50.
Protocol:	Select the protocol used by the service.
Private Port:	The port that will be used on your internal network.
Public Port:	The port that will be accessed from the Internet.
Schedule:	Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.
Save:	Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

Virtual Servers List

Entries on this list can be enabled/disabled by toggling the Enable checkbox. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Special Applications

The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a 'trigger' port or port range. Special Applications rules apply to all computers on your internal network.

Application Level Gateway (ALG) Configurations

Here you can enable or disable ALG's. Some protocols and applications require special handling of the IP payload to make them work with network address translation (NAT). Each ALG provides special handling for a specific protocol or application. A number of ALGs for common applications are enabled by default.

PPTP: Allows multiple machines on the LAN to connect to their corporate network using PPTP protocol.

IPSec VPN: Allows multiple VPN clients to connect to their corporate network using IPSec. Some VPN clients support traversal of IPSec through NAT. This ALG may interfere with the operation of such VPN clients. If you are having trouble connecting with your corporate network, try turning this ALG off. *Please check with the system adminstrator of your corporate network whether your VPN client supports NAT traversal.*

RTSP: Allows applications that use Real Time Streaming Protocol to receive streaming media from the internet. QuickTime and Real Player are some of the common applications using this protocol.

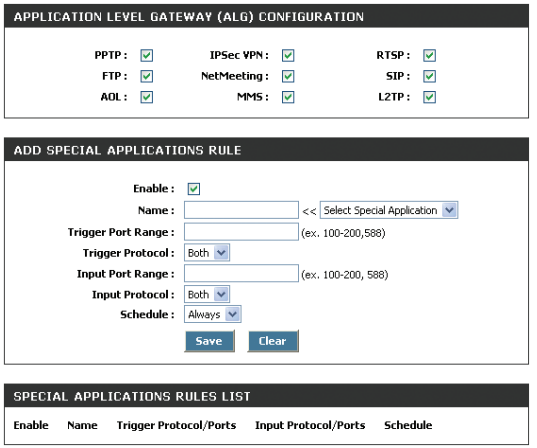
FTP: Allows FTP clients and servers to transfer data across NAT. Refer to the Advanced -> Virtual Server page if you want to host an FTP server.

NetMeeting: Allows Microsoft NetMeeting clients to communicate across NAT. Note that if you want your buddies to call you, you should also set up a virtual server for NetMeeting. Refer to the Advanced -> Virtual Server page for information on how to set up a virtual server.

SIP: Allows devices and applications using VoIP (Voice over IP) to communicate across NAT. Some VoIP applications and devices have the ability to discover NAT devices and work around them. This ALG may interfere with the operation of such devices. If you are having trouble making VoIP calls, try turning this ALG off.

MMS: Allows Windows Media Player, using MMS protocol, to receive streaming media from the internet.

L2TP: Allows multiple machines on the LAN to connect to their corporate network using the L2TP protocol.



Advanced > Special Applications

Add/Edit Special Applications Rule

The Special Application section is used to open single or multiple ports on your router when the router senses data sent to the Internet on a “trigger” port or port range. Special Applications rules apply to all computers on your internal network.

Rule Name:	Enter a name for the Special Application Rule, for example **Game App**, which will help you identify the rule in the future. You can also select from a list of common applications, and the remaining configuration values will be filled in accordingly.
Trigger Port Range:	Enter the outgoing port range used by your application.
Trigger Port Protocol:	Select the outbound protocol used by your application.
Input Port Range:	Enter the port range that you want to open up to Internet traffic.
Input Port Protocol:	Select the protocol used by the Internet traffic coming back into the router through the opened port range.
Schedule:	Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.
Save:	Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

Special Applications Rules List

Entries on this list can be enabled/disabled by toggling the Enable checkbox. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you’ve completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Gaming

The Gaming section is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats:

Add/Edit Game Rule

Rule Name: Give the Gaming Rule a name that is meaningful to you, such as Game Server. You can also select from a list of pre-defined rules for many popular games. If you have any trouble with pre-defined rules, verify whether the port values have changed since the list was created. You also must fill in the IP address field.

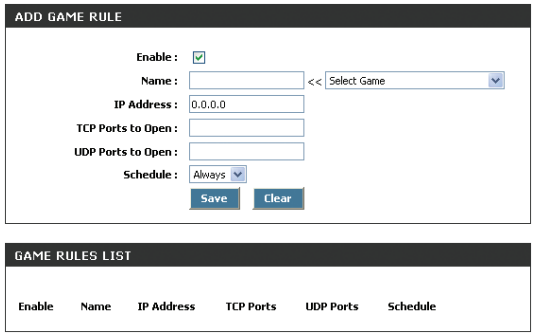
IP Address: Enter the local network IP address of the system hosting the game server, such as 192.168.0.50.

TCP Ports To Open: Enter the TCP ports to open, such as 6159-6180, 99

UDP Ports To Open: Enter the UDP ports to open, such as 6159-6180, 99

Schedule: Select a schedule for when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Tools -> Schedules screen and create a new schedule.

Save: Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.



Advanced > Gaming

Game Rules List

Entries on this list can be enabled/disabled by toggling the Enable checkbox. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

GameFuel™

The GameFuel™ option helps improve your network gaming performance by prioritizing applications. By default the GameFuel settings are disable and application priority is not automatically classified.

GameFuel™ Setup

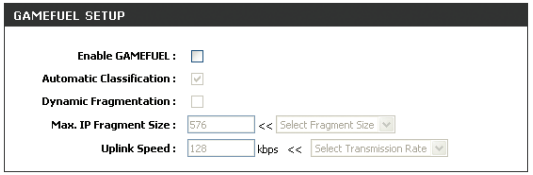
Enable GameFuel: This option is disabled by default. Enable this option for better performance and experience with online games and other interactive applications, such as VoIP.

Automatic Classification: This option is enabled by default when the GameFuel option is enabled. This option will allow your router to automatically determine which programs should have network priority.

Dynamic Fragmentation: This option should be enabled when you have a slot Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones.

Max. IP Fragment Size: If Dynamic Fragmentation is enabled, you can fine tune the fragment size. The default value is 576. Select a smaller size if you have a slow uplink and VoIP quality is not optimal; select a larger size for faster uplinks.

Uplink Speed: The speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISP's often speed as a download/upload pair. For example, 1.5Mbits/284Kbits. Using this example, you would enter 284. Alternatively you can test your uplink speed with a service such as www.dslreports.com.



Advanced > GameFuel

Add/Edit GameFuel™ Rule

Automatic classification should be adequate for most applications. GameFuel rules identify a specific message flow and assign priority to that flow.

Name:	Create a name for the rule that is meaningful to you.
Priority:	The priority of the message flow is entered here. O receives the highest priority (most urgent) and 255 receives the lowest priority.
Protocol:	The protocol used by the messages.
Source IP Range:	The rule applies to a flow of messages whose LAN-side IP address is within the range set here.
Source Port Range:	The rule applies to a flow of messages whose LAN-side port number is within the range set here.
Destination IP Range:	The rule applies to a flow of messages whose WAN-side IP address is within the range set here.
Destination Port Range:	The rule applies to a flow of messages whose WAN-side port number is within the range set here.
Save:	Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

GameFuel Rules List

Entries on this list can be enabled/disabled by toggling the Enable checkbox. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Routing

Add/Edit Route

Adds a new route to the IP routing table or edits an existing route.

Enable: Specifies whether the entry will be enabled or disabled.

Destination IP: The IP address or network that the packets will be attempting to access

Note: 192.168.1.0 with a Netmask of 255.255.255.0 means traffic will be routed to the entire 192.168.1.x network.

Netmask: Used to specify which portion of the Destination IP signifies the network trying to be accessed and which part signifies the host that the packets will be routed to

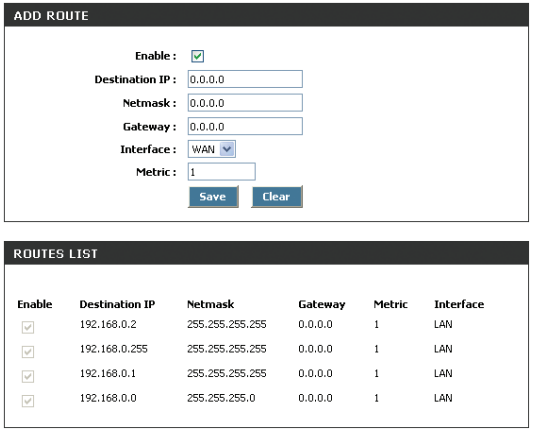
Note: 255.255.255.255 is used to signify only the host that was entered in the Destination IP field.

Gateway: Specifies the next hop to be taken if this route is used. A gateway of 0.0.0.0 implies there is no next hop, and the IP address matched is directly connected to the router on the interface specified: LAN or WAN.

Interface: Specifies the interface, LAN or WAN, that the IP packet must use to transit out of the router when this route is used.

Metric: The amount of hops it will take to reach the Destination IP or network. A hop is considered to be traffic passing through a router from one network to another. If there is only one router between your network and the Destination network, then the Metric value would be 1.

Save: Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.



Advanced > Routing

Route List

This section shows the current routing table entries. Certain required routes are predefined and cannot be changed. Entries on this list that can modified can be enabled/disabled by toggling the Enable checkbox. Editable entries can be modified by clicking on the paper and pencil icon. To delete an editable entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Access Control

The Access Control section allows you to control access in and out of your network. Use this feature as Parental Controls to only grant access to approved sites, limit web access based on time or dates, and/or block access from applications like P2P utilities or games.

Enabled

By default the Access Control feature is disabled. If you enable Access Control, every device on the LAN must either have a static IP address (that is one that is not in the DHCP range) or must be in the Static DHCP Client List (see Basic > DHCP).

When Access Control is disabled, every device on the LAN is permitted to access the Internet. However, if you enable Access Control, every device on the LAN that needs to access the Internet must have an Access Control rule that explicitly permits it to access the Internet. Devices that do not have an Access Control Rule cannot access the Internet. When Access Control is enabled, the options below will appear:

Add/Edit Access Control Rule

Policy Name: Create a name for this access control policy that is meaningful to you. Typically this would be a system name or user name such as Rob's PC.

Machine IP Address: The local network IP address of the machine that you want the access control rule to apply to. Example: 192.168.0.50. Make sure that this is a static IP address or the system is in the static DHCP Client list (See Basic > DHCP).

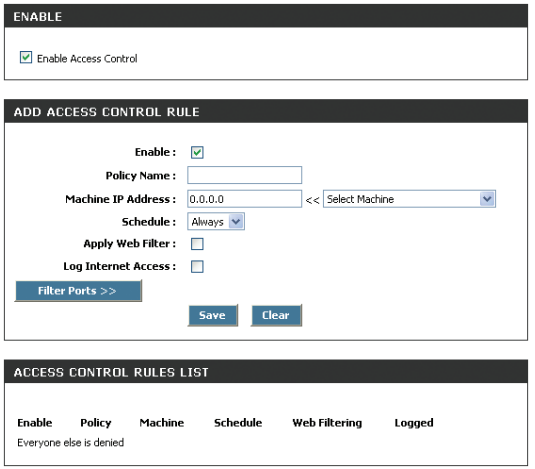
Schedule: Select a schedule of times when you want the policy to apply. If you do not see the schedule you need in the list of schedules, go to the Tools > Schedules screen and create a new schedule.

Apply Web Filter: With this option enabled, the specified system will only have access to the Web sites listed in the Web filter section.

Log Internet Access: If this option is enabled, all of the Web sites visited by the specified machine will be logged.

Filter Ports: By clicking the Filter Ports >> button you can specify that the rule enables access only to specific IP addresses and ports.

Save: Saves the new or edited access control rule in the Access Control Rules List. Repeat the process, creating an Access Control Rule for each of the devices on your LAN that needs access to the Internet. When finished updating Access Control Rules, you must still click the Save Settings button at the top of the page to make changes effective and permanent.



Advanced > Access Control

Access Control Rules List

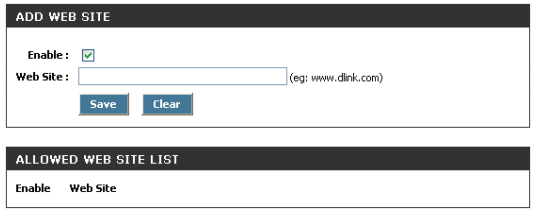
This section shows the current Access Control rules. Any device that does not have a rule, cannot access the Internet. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Web Filter

The Web Filter section is where you add the Web site to be used for Access Control.

Add/Edit Web Site

This field is where you can add Web sites to the Allowed Web List. The Allowed Web List is used for systems that have the Web filter option enabled in Access Control.



Advanced > Web Filter

Enable: Entries in the Allowed Web Site List can be activated or deactivated with this checkbox. New entries are activated by default.

Web Site: Enter the URL (address) of the web site that you want to allow (such as **google.com**). Enter the most inclusive domain name. For instance, entering dlink.com will give you access to www.dlink.com and support.dlink.com. **Do not enter** the **http://** preceding the URL.

Note: Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all of the web sites used to construct a page. For example, to access my.yahoo.com, you must enable access to yahoo.com, yimg.com, and doubleclick.net.

Save: Saves the new or modified Allowed Web Site in the Allowed Web Site List. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

Allowed Web Site List

This section lists the currently allowed web sites. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Mac Address Filters

The MAC (Media Access Controller) Address filter section is used to control network access based on the MAC Address of the network adapter. A MAC address is a unique ID assigned by the manufacturer of a networking device. This feature can be configured to ALLOW or DENY network/ Internet access.

Filter Settings

MAC Filter Enabled: When this is enabled, depending on the mode selected, computers are granted or denied network access based on their MAC address.

Mode: When Allow is selected, only computers with MAC addresses listed in the MAC Address List are granted network access. When Deny is selected, any computer with a MAC address listed in the MAC Address List

Filter Wireless Clients: When this is selected, the MAC address filters will be applied to wireless network clients.

Filter Wired Clients: When this is selected, the MAC address filters will be applied to wired network clients.

Advanced > MAC Address Filter

Add MAC Address

Enable: MAC address entries are activated or deactivated with this checkbox.

MAC Address: Enter the MAC address of the desired computer or connect to the router from the desired computer and click Copy Your PC's MAC Address button.

Save: Saves the new or modified MAC address in the MAC Address List. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

MAC Address List

This section lists the current MAC address filters. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Firewall

A firewall protects your network from the outside world. The D-Link Gaming Router offers a firewall type functionality. The SPI feature helps prevent cyber attacks. Sometimes you may want a computer exposed to the outside world for certain types of applications. If you choose to expose a computer, you cam enable DMZ. DMZ is short for Demilitarized Zone. This option will expose the chosen computer completely to the outside world.

Firewall Settings

Enable SPI: SPI (Stateful Packet Inspection, also known as dynamic packet filtering) helps to prevent cyber attacks by tracking more state per session. It validates that the traffic passing through the session conforms to the protocol. When SPI is enabled, the extra state information will be reported on the Status > Active sessions page.

Enable DMZ: If an application has trouble working from behind the router, you can expose one computer to the Internet and run the application on that computer.

Note: Placing a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

DMZ IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains it's IP address automatically using DHCP, be sure to make a static reservation on the Basic > DHCP page so that the IP address of the DMZ machine does not change.

Advanced > Firewall

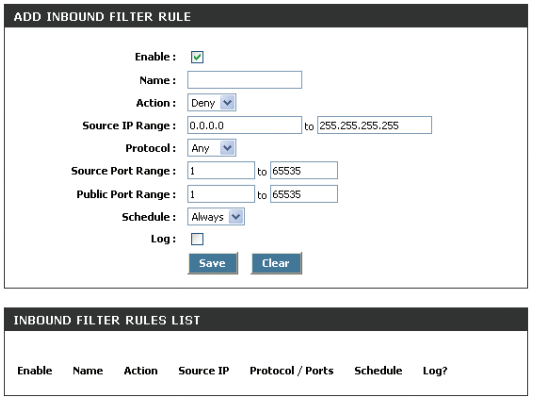
After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Inbound Filters

The Inbound Filters option is an advanced method of controlling data received from the Internet. With this feature you can configure inbound data filtering rules that control data based on IP Address, Protocol, and/or Port.

The Inbound Filter option is best suited for custom applications. For most applications you should use Virtual Server, Special Applications, or the Gaming section to create rules that will allow applications to communicate through the router.

Add/Edit Inbound Filter Rule



Advanced > Inbound Filters

Enable: Enables inbound filtering.

Name: Enter a name for the rule that is meaningful to you.

Action: The rule can be set to either allow or deny applicable messages.

Source IP Range: Defines the range of Internet addresses this rule applies to.

Protocol: Select the protocol used for this rule.

Source Port Range: Enter the range of ports that this rule applies to.

Public Port Range: Enter the range of WAN side ports associated with the servers on the LAN that this rule applies to.

Schedule: Select a schedule for the times when this rule should be in effect. If you do not see the schedule you need in the list of schedules, go to the Tools > Schedules screen and create a new schedule.

Log: Check this option if you want the router to add an entry to the log whenever a rule is enforced.

Save: Saves the new rule or modified existing rule to the Rules list. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.

Inbound Filter Rules List

This section lists the current Inbound Filter rules. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Configuring an Inbound Filter Rule

When the Rule List is empty or none of the rules are enabled, all inbound data that corresponds to a connection that originated from inside the router or which corresponds to a Virtual Server, Gaming, or Special Application Rule is ALLOWED by default.

When rules are configured, the router compares incoming data packets against the rules in the list. It is very important to understand that the router examines each rule one by one in the order that they are listed in the Rule list until it finds a match. The packet will either be DENIED (Dropped) or ALLOWED. Once a match has been made, no further rules will be examined for that packet. If no rules match the data packet, it is ALLOWED. This means that to allow only a specific subset of traffic usually requires more than one rule to be entered.

Example:

You have configured a game server, using the Advanced > Gaming page, to play HALO: Combat Evolved with some friends. You would like to limit the access to your network and server to specific times of the day and only to your friends.

Next you would define a schedule on the Tools > Schedule page, called Gametime, which specifies a schedule of Friday and Saturday between 7PM and 11PM.

All of your friends use the same service provider and have IP addresses 67.150.220.117, 67.150.231.43, and 67.150.231.75. You have an option of defining a set of rules to match each one of these addresses individually or you may just decide that using an IP range that covers all of them is sufficient for your needs.

The first rule is to configure a DENY rule that will catch all of the traffic that arrives on these ports but does not match data from the sources you want to have access to your network. It is important to enter the DENY rule first since all subsequent rules will be added higher in the list and will be checked first. It should look similar to the figure on the right.

Notice that it covers all Source IP Address, Source Ports, and Times (Always), but is specifically tied to the Public Ports defined in the Game Rule List. This is because you do not want to accidentally block traffic for other applications. It is a good idea to turn on the log for this rule so that you can check in the log for anything that is filtered inappropriately.

Next configure the ALLOW rules. In the example on the right, two rules are used to cover the three IP addresses.

GAME RULES LIST

Enable	Name	IP Address	TCP Ports	UDP Ports	Schedule
☑	Halo: Combat Evolved	192.168.0.20		2302, 2303	Always

INBOUND FILTER RULES LIST

Enable	Name	Action	Source IP	Protocol / Ports	Schedule	Log?
☑	HALO: CE DENY	Deny	0.0.0.0-255.255.255.255	UDP/ 1-65535/ 2302-2303	Always	Yes

INBOUND FILTER RULES LIST

Enable	Name	Action	Source IP	Protocol / Ports	Schedule	Log?
☑	HALO: CE 2	Allow	67.150.231.1-67.150.231.255	UDP/ 1-65535/ 2302-2303	GAMETIME	No
☑	HALO: CE 1	Allow	67.150.220.117-67.150.220.117	Any/ 1-65535/ 2302-2303	GAMETIME	No
☑	HALO: CE DENY	Deny	0.0.0.0-255.255.255.255	UDP/ 1-65535/ 2302-2303	Always	Yes

Advanced Wireless

Advanced Wireless Settings

Fragmentation Threshold: This setting should remain at its default setting of 3200. If you experience a high packet error rate, you may slightly adjust your "Fragmentation" value somewhere in the between the recommended range of 256 to 3200. Setting the Fragmentation value too low may result in poor performance.

RTS Threshold: This setting should remain at its default setting of 3200. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

Beacon Period: Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Period value between 20 and 1000. The default value is set to 100 milliseconds.

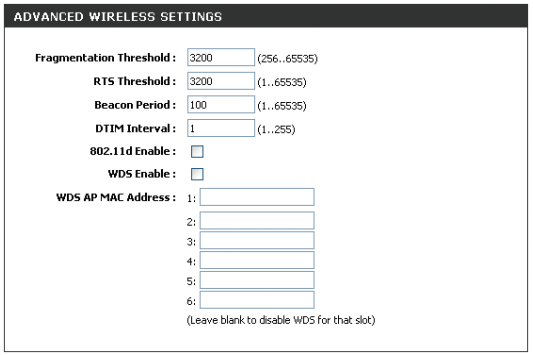
DTIM Interval: The default value is set to 1. Valid settings are between 1 and 255. A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients hear the beacons and awaken to receive the broadcast and multicast messages.

802.11d Enable: This enables 802.11d opration. **802.11d** is a wireless specification developed to allow implementation of wireless networks in countries that cannot use the 802.11 standard. This feature should only be enabled if you are in a country that requires it.

WDS Enable: When WDS is enabled, this access point functions as a wireless bridge and is able to wirelessly communicate with other AP's via WDS links.

Note: WDS is incompatible with WPA. Both features cannot be used at the same time. A WDS link is bidirectional so this AP must know the MAC address (creates the WDS link) of the other AP, and the other AP must have a WDS link back to this AP (the router).

WDS AP MAC Address: Specifies one-half of the WDS link. The other AP must also have the MAC address of this AP (the router) to create the WDS link back to the router.



Advanced > Advanced Wireless

Tools

Admin

The Admin option is used to set a password for access to the Web-based management. By default there is no password configured. It is highly recommended that you create a password to keep your new router secure.

Password

Password: Enter a password the will grant access to the Web-based management interface.

Administration

Gateway Name: The name of the router can be changed here.

Remote Management: Enabling this allows you to manage the router from anywhere with an Internet connection.

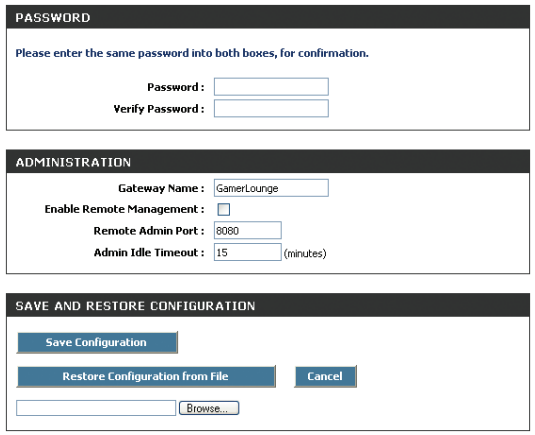
Remote Management Server Port: The port that will be accessed from the Internet.

Admin Idle Timeout: The amount of time before the administration session is closed when there is no activity. ***Note: This applies to local or remote administration.***

Save and Restore Configuration

Save Settings: This option allows you to save the router configuration to a file on your computer. Be sure to save the configuration before performing a firmware upgrade.

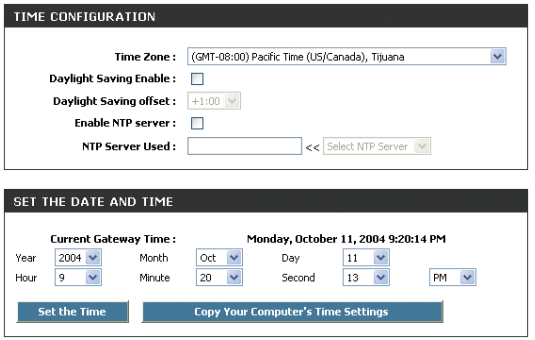
Restore Settings: Use this option to load previously saved router configuration settings.



Tools > Admin

Time

The Time Configuration option allows you to configure, update, and maintain the correct time on the internal system clock. From this section you can set the time zone that you are in and set the Time Server. Daylight Saving can also be configured to automatically adjust the time when needed.



Tools > Time

Time Configuration

Time Zone: Select your local time zone from pull down menu.

Daylight Saving Enable: Check this option if your location observes daylight saving time.

Daylight Saving Offset: Select the time offset if your location observes daylight saving time.

Synchronize time with NTP server: Select this option if you want the router's clock synchronized to a Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate

NTP Server: Select a Time Server for synchronization. You can type in the address of a time server or select one from the list. If you have trouble using one server, select another.

Set the Date and Time

If you do not have the NTP Server option in effect, you can either manually set the time for your router here or you can click the Copy Your Computer's Time Settings button to copy the time from the computer you are using (Note: Be sure the computer's time is set correctly).

Note: If the router loses power for any reason, it cannot keeps its clock running and will not have the correct time when it is started again. To maintain the correct time for schedules and logs, either you must enter the correct time after you restart the router or you must enable the NTP Server option.

Schedules

Schedules can be created for use with enforcing rules. For example, if you want to restrict web access to Mon-Fri from 3pm to 8pm. You could create a schedule selecting Mon, Tue, Wed, Thu, and Fri and enter a Start Time of 3pm and End Time of 8pm.

Add/Edit Schedule Rule

Schedule Name: Name the schedule, such as Weekday rule.

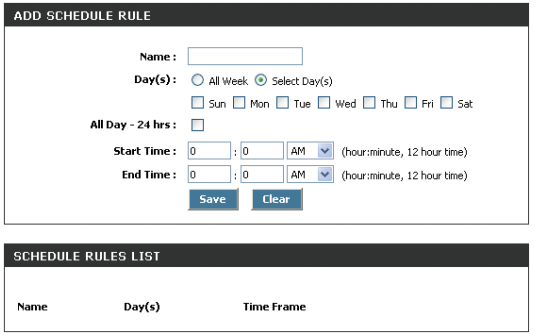
Day(s): Place a checkmark in the boxes for the desired days or select the All Week radio button to select all seven days of the week.

All Day: Select this option if you want this schedule in effect all day for the selected day(s).

Start Time: If you don't use the All Day option, then you enter in the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email events are triggered only by the start time.

End Time: The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not used for email events.

Save: Saves the new or modified Schedule in the Schedule Rules List. When you are done editing the settings, you must click the Save Settings button at the top of the page to make the changes effective and permanent.



Tools > Schedules

Schedule Rules List

This list displays all of the currently defined schedules. Entries can be modified by clicking on the paper and pencil icon. To delete an entry, click on the trash can icon. After you've completed all modifications or deletions, you must click the **Save Settings** button at the top of the page to save your changes. The router must reboot before new settings will take effect. You will be prompted to **Reboot the Device** or **Continue**. If you need to make additional settings changes, click **Continue**. If you are finished with your configuration settings, click the **Reboot the Device** button.

Syslog

This section allows you to archive your log files to a Syslog Server.

Archive to Syslog: Enable this option to output the router logs to a Syslog Server on your network.

Syslog Server IP Address: Enter the IP address of the Syslog Server.

Tools > Syslog

Email

The Email feature can be used to send the system log files, router alert messages, and firmware update notification to your email address.

Email Settings

Enable Email notification: When this option is enabled, router activity logs are e-mailed to a designated email address.

From Email address: This email address will appear as the sender when you receive a log file or firmware upgrade notification via email.

To Email address: Enter the email address where you want the email sent.

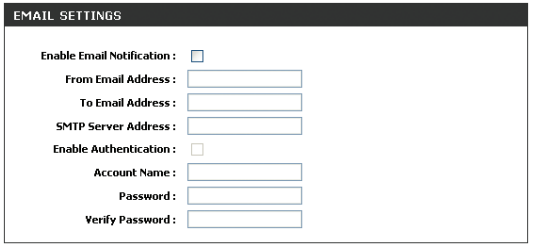
SMTP Server Address: Enter the SMTP server address for sending email.

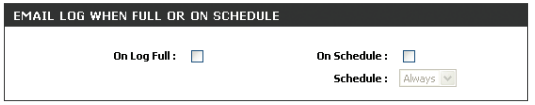
Enable Authentication: If your SMTP server requires authentication, select this option.

Account Name: Enter your account for sending email.

Password: Enter the password associated with the account.

Verify Password: Re-type the password associated with the account.





Tools > Email

Email Log When Full or on Schedule

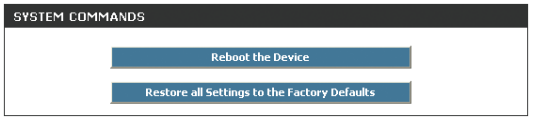
On Log Full: When this option is selected, logs will be sent via email when the log is full.

On Schedule: Selecting this option will send the logs via email according to schedule.

Schedule: This option is enabled when On Schedule is selected. You can select a schedule from the list of defined schedules. To create a schedule, go to Tools > Schedules.

System

The System Settings section allows you to reboot the device or restore the router to the factory default settings. Restoring the unit to the factory default settings will erase all settings including any rules that you've created.



Tools > System

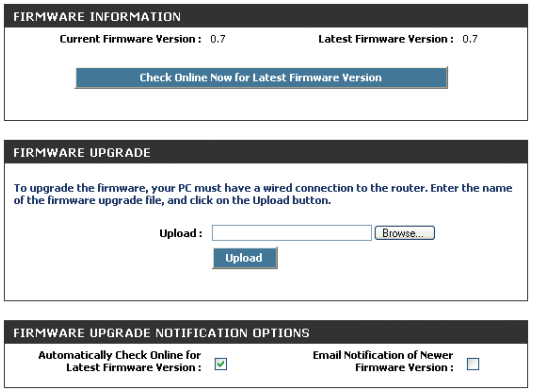
System Commands

Reboot the Device: This will restart the router. Useful for restarting when you are not near the device.

Restore all Settings to the Factory Defaults: This option will restore all configuration settings back to the factory defaults. Any settings that have not been saved will be lost. If you want to save your router configuration settings, you can do so from the Admin page.

Firmware

The Firmware Upgrade section can be used to update your router to the latest firmware code to improve functionality and performance. To check for the latest firmware, click the Check Online Now button. If you would like to be notified when new firmware is released, place a checkmark in the box next to Email Notification of Newer Firmware Version.



Tools > Firmware

Firmware Information

This section displays the Current Firmware Version and the Latest Firmware Version. To verify the latest firmware version, the gaming router checks the Internet. To check for the latest version, click the **Check Online Now for Latest Firmware Version** button.

Firmware Upgrade

To upgrade the firmware, follow these steps:

1. Click the [Browse] button to locate the D-Link upgrade file on your computer.
2. Once you have found the file to be used, click the Upload button below to start the firmware upgrade process.
3. Wait for the router to reboot
4. Confirm updated firmware revision on status page

Current Firmware Version: 2.37

Firmware Date: Mon, 23 Feb 2004

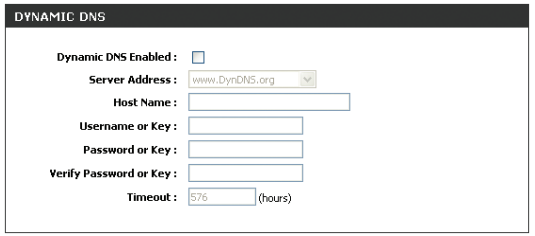
Firmware Upgrade Notification Options

Automatically Check Online for Latest Firmware Version: When this option is enabled, your router will check online periodically to see if a newer version of the firmware is available.

Email Notification of Newer Firmware Version: When this option is enabled, an email will be sent to the email address configured in the email section whenever new firmware is available.

Dynamic DNS

The DDNS feature allows you to host a server (Web, FTP, Game Server, etc…) using a domain name that you have purchased (www.whateveryournameis.com) with your dynamically assigned IP address. Most broadband Internet Service Providers assign dynamic (changing) IP addresses. Using a DDNS service provider, your friends can enter in your domain name to connect to your server no matter what your IP address is.



Tools > Dynamic DNS

Dynamic DNS Enabled: Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider.

Server Address: Select a dynamic DNS service provider from the pull-down list.

Host Name: Enter your host name.

Username or Key: Enter the username or key provided by your service provider.

Password or Key: Enter the password or key provided by your service provider.

Verify Password or Key: Re-type the password or key provided by your service provider.

Timeout: The time between periodic updates to the Dynamic DNS, if your dynamic IP address has not change. The timeout period is entered in hours.

Note: Option will disable it self if Username and Password or keys are incorrect.

Status

The Status items are mainly informational.

Device Info

The Device Info page displays your Router settings. Options cannot be modified from this page.

General

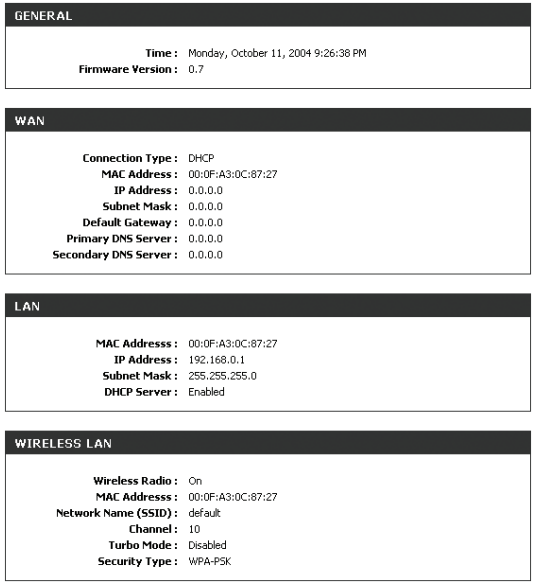
Time:	Displays the time and date that the router is set to.
Firmware Version:	Displays the currently loaded firmware version.

WAN

Connection Type:	The Internet connection type that is being used.
MAC Address:	The MAC address that is seen over the Internet.
IP Address:	The IP address being used on the WAN port.
Subnet Mask:	The subnet mask used on the WAN port.
Default Gateway:	The default gateway of the WAN port.
Primary DNS Server:	The Primary DNS Server address.
Secondary DNS Server:	The Secondary DNS Server address.

LAN

MAC Address:	The MAC address displayed for your local area network.
IP Address:	The IP address of the router on your local area network.
Subnet Mask:	The subnet mask of the router on your local area network.
DHCP Server:	Indicates if the router is acting as a DHCP server on the local area network.



Status > Device Info

Wireless LAN

Wireless Radio:	Indicates whether wireless networking is on or off.
MAC Address:	The MAC address displayed for your wireless network.
Network Name (SSID):	The Network Name, also referred to as SSID, of your wireless network.
Channel:	The channel being used by the router for broadcasting on the wireless network.
Turbo Mode:	Indicates whether Turbo Mode is enabled or disabled.
Security Type:	Indicates the type of wireless security being used.

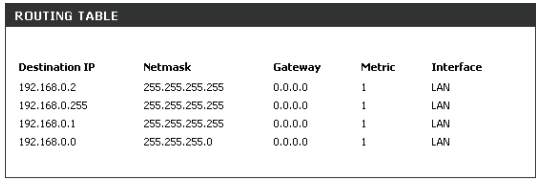
Wireless

This screen displays the number of wireless clients that are connected to the router, the MAC address of each system connecting wirelessly, and the IP address of each system connecting wirelessly.

Routing

This page displays the routing details configured for the router.

A gateway value of 0.0.0.0 means there is no next hop. The IP address is directly connected to the router on the interface specified, LAN or WAN. A value of 0.0.0.0 in both the destination IP and netmask means that this is the default route.


ROUTING TABLE

Destination IP	Netmask	Gateway	Metric	Interface
192.168.0.2	255.255.255.255	0.0.0.0	1	LAN
192.168.0.255	255.255.255.255	0.0.0.0	1	LAN
192.168.0.1	255.255.255.255	0.0.0.0	1	LAN
192.168.0.0	255.255.255.0	0.0.0.0	1	LAN

Status > Routing

Logs

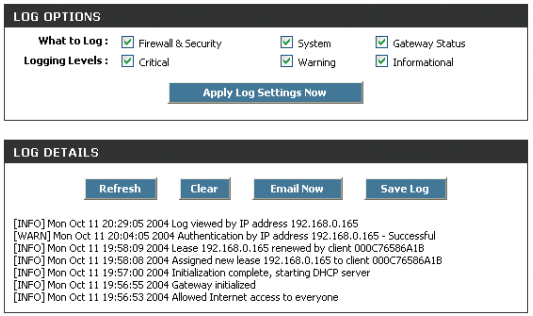
The router automatically logs (records) events of possible interest in it's internal memory. If there isn't enough internal memory for all events, logs of older events are deleted but logs of the latest events are retained. The Logs option allows you to view the router logs. You can define what types of events you want to view and the level of the events to view. This router also has external Syslog Server support so you can send the log files to a computer on your network that is running a Syslog utility.

Log Options

What to View: You can select the types of messages that you want to display from the log. Firewall & Security, System, and Router Status messages can be selected.

View Levels: There are three levels of message importance: Informational, Warning, and Critical. Select the levels that you want displayed in the log.

Apply Log Settings Now: Will filter the log results so that only the selected options appear.



Status > Logs

Log Details

Refresh: Updates the log details on the screen so it displays any recent activity.

Clear: Clears all of the log contents.

Email Now: This option will send a copy of the router log to the email address configured in the Tools > Email screen.

Save Log: This option will save the router to a log file on your computer.

Statistics

Network Traffic Stats

Refresh Statistics: Updates the screen with the latest router statistics.

Clear Statistics: Clears all of the values on the screen.

LAN Statistics

Sent:	The number of packets transmitted to the local area network.
Received:	The number of packets received from the local area network.
TX Packets Dropped:	The number of transmit packets dropped on the local area network.
RX Packets Dropped:	The number of receive packets dropped on the local area network.
Collisions:	The number of collisions on the local area network.
Errors:	The number of errors occuring on the local area network.

WAN Statistics

Sent:	The number of packets transmitted to the Internet.
Received:	The number of packets received from the Internet.
TX Packets Dropped:	The number of transmit packets sent to the WAN port that were dropped.
RX Packets Dropped:	The number of receive packets sent to the WAN port that were dropped.
Collisions:	The number of collisions involving packets intended for the WAN port.
Errors:	The number of errors occuring with packets intended for the WAN port.

Wireless Statistics

Sent:	The number of packets sent to the wireless network.
Received:	The number of packets received from the wireless network.
TX Packets Dropped:	The amount of transmit packets dropped.
Errors:	The number of errors relating to packets to/from the wireless network.

Active Sessions

The Active Session page displays the full details of active sessions to your router.

Appendix

Securing Your Network

1. Change Admin Password

Changing the password to access your new router is the first step in securing your network. This can done through the Wizard or on the Admin Page of the Tools tab. There is no password by default and hackers will know this when trying to access your network. Make sure that the password you choose is not commonly known or something that is easy to guess such as your last name or your pet's name. Try using a combination of letters and numbers to deter intruders from hacking into your network. Your private information should be kept private.

2. Disable DHCP and use Static IP addresses or Use Static DHCP and limit scope to the amount of users on your network.

In the event that an intruder manages to gain access to your network, having DHCP enabled makes it easier for the intruder to access other computers on your network. There are two methods for getting around this. One is to disable DHCP and use static IP addressing on all the devices connected to your network. This would mean that the intruder would have to know what IP network your devices are on in order to access them. The second way is to change the scope of the DHCP server to only include enough IP addresses for the devices in your network. You can then use the Static DHCP feature of the router to assign an IP address to each device on your network. Static DHCP still dynamically assigns an IP address to your network devices but only allows for those defined devices to obtain an IP address.

3. Change the default LAN IP address

Change the default LAN IP address from 192.168.0.1 to an alternate IP address. There are 3 ranges of IP addresses that have been reserved for use on Private Networks.

10.0.0.0 - 10.255.255.255 (10.0.0.0/8)

172.16.0.0 - 172.31.255.255 (172.16.0.0/12)

192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

D-Link routers use 192.168.0.1 as their default LAN IP address. Choosing an alternate IP address lessens the probabilty of an intruders knowing what IP network your devices are on.

4. Changing the Wireless Network Name (SSID - used for wireless devices only)

It is always a good idea to change the wireless network name (SSID) from the default value. Leaving it in the default state is usually a good indication to intruders that all settings (including security) are probably defaults. This setting identifies your wireless network. Make sure that the name you choose is not commonly known or something that is easy to guess. Try using a combination of letters and numbers to add complexity to it.

5. Set the Visibility Status to Invisible

Wireless routers typically broadcast the wireless network name (SSID) to users attempting to connect to a wireless network. By setting the Visibility Status to Invisible, all devices attempting to connect to the router will need to know the wireless network name (SSID) in order to connect.

6. Enable WPA Personal or Enterprise

Along with changing the wireless network name and setting the visibility status to invisible, we highly recommended that you enable some sort of encryption feature. There are different methods of securing wireless transmissions, but the most effective is WPA-Personal and WPA-Enterprise. WPA-Personal is easier to configure but does not offer the extensive level of security that WPA Enterprise does. If you have the infrastructure to support WPA Enterprise, we recommend that you use this method. If not, then WPA-Personal will suffice.

7. Set up MAC Filtering

Each networking device (router, access point, wireless card, etc.) on a network contains a unique hexadecimal number that identifies that specific product. This number is referred to as a MAC address. MAC filtering allows you to create a list of the MAC address of each device on your network and only allows these specific devices to associate with your network. With this feature enabled, devices attempting to connect to your network with a MAC address that is not in the list you created, will be denied access.

Glossary

A

Access Control List - ACL. Database of network devices that are allowed to access resources on the network.

Access Point - AP. Device that allows wireless clients to connect to it and access the network

Ad-hoc network - Peer-to-Peer network between wireless clients

Address Resolution Protocol - ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

ADSL - Asymmetric Digital Subscriber Line

Advanced Encryption Standard - AES. Government encryption standard

Alphanumeric - Characters A-Z and 0-9

Antenna - Used to transmit and receive RF signals.

AppleTalk – A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol – AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer - 7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII - American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation – The loss in strength of digital an analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication –To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing - APIPA. An IP address that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible - The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth - The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System – BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud – Data transmission speed

Bit rate – The amount of bits that pass in given amount of time

bit/sec – bits per second

BOOTP – Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck – A time during processes when something causes the process to slowdown or stop all together

Broadband – A wide band of frequencies available for transmitting data

Broadcast – Transmitting data in all directions at once

Browser – A program that allows you to access resources on the web and provides them to you graphically

C

Cable modem – A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus – A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

Carrier Sense Multiple Access/Collision Avoidance – CSMA/CA

Carrier Sense Multiple Access/Collision Detect – CSMA/CD

CAT 5 – Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client – A program or user that requests data from a server

Collision – When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie – Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD – Carrier Sense Multiple Access/Collision Detection

D

Data – Information that has been translated into binary do that it can be processed or moved to another device

Data Encryption Standard – Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Data-Link layer – The second layer of the OSI model. Controls the movement of data on the physical link of a network

Database – Organizes information so that it can be managed updated, as well as easily accessed by users or applications.

DB-25 – A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9 – A 9 pin connector for RS-232 connections

dBd - decibels related to dipole antenna

dBi - decibels relative to isotropic radiator

dBm - decibels relative to one milliwatt

Decrypt – To unscramble an encrypted message back into plain text

Default – A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone – DMZ. A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP – Dynamic Host Configuration Protocol. Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that requests them

Digital certificate – An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum – DSSS. Modulation technique used by 802.11b wireless devices

DNS – Domain Name System. Translates Domain Names to IP addresses

DOCSIS – Data Over Cable Service Interface Specifications. The standard interface for cable modems

Domain name – A name that is associated with an IP address

Download – To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL – Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex – Sending and Receiving data transmissions at the sane time

Dynamic DNS service – DDNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports DDNS, whenever the IP address changes

Dynamic IP address – IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP – Extensible Authentication Protocol

Email – Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption – Converting data into cyphertext so that it cannot be easily read

Enterprise – Large organizations that use computers

Ethernet – The most widely used technology for Local Area Networks.

F

Fiber optic – A way of sending data through light impulses over glass or plastic wire or fiber

File server – A computer on a network that stores data so that the other computers on the network can all access it

File sharing – Allowing data from computers on a network to be accessed by other computers on the network will different levels of access rights

Firewall – A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware – Programming that is inserted into a hardware device that tells it how to function

Fragmentation – Breaking up data into smaller pieces to make it easier to store

FTP – File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex – Sending and Receiving data at the same time

G

Gain – The amount an amplifier boosts the wireless signal

Gateway – A device that connects your network to another, like the internet

Gbps – Gigabits per second

Gigabit Ethernet – Transmission technology that provides a data rate of 1 billion bits per second

Graphical user interface – GUI

H

H.323 – A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex – Data cannot be transmitted and received at the same time

Hashing – Transforming a string of characters into a shorter string with a predefined length

Hexadecimal – Characters 0-9 and A-F

HomePNA – Networking over telephone lines

HomeRF – Networking standard that combines 802.11b and DECT (Digital Enhanced Cordless Telecommunication) that provides speeds up to 1.6 Mbps and a distance of 150 ft using a Frequency Hopping transmission method

Hop – The action of data packets being transmitted from one router to another

Host – Computer on a network

HTTP – Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS – HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub – A networking device that connects multiple devices together

I

ICMP – Internet Control Message Protocol

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IGMP – Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS – Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE – Internet Key Exchange is used to ensure security for VPN connections

Infrastructure – In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet – A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer – A World Wide Web browser created and provided by Microsoft

Internet Protocol – The method of transferring data from one computer to another on the Internet

Internet Protocol Security – IPsec provides security at the packet processing layer of network communication

Internet Service Provider – An ISP provides access to the Internet to individuals or companies

Interoperability – The ability for products to interact with other products without much customer interaction

Intranet – A private network

Intrusion Detection – A type of security that scans a network to detect attacks coming from inside and outside of the network

IP – Internet Protocol

IP address – A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec – Internet Protocol Security

IPv6 – Internet Protocol Version 6 uses 128-bit addresses and was developed to solve the problem that we face of running our of IP version 4 addresses

IPX – Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP – Internet Service Provider

J

Java – A programming language used to create programs and applets for web pages

K

Kbps – Kilobits per second

Kbyte - Kilobyte

Kerberos – A method of securing and authenticating requests for services on a network

L

LAN – Local Area Network

Latency – The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED - Light Emitting Diode

Legacy – Older devices or technology

Local Area Network – A group of computers in a building that usually access files from a server

M

MAC address – A unique hardware address for devices on a Local Area Network

MDI – Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX - Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

Megabit - Mb

Megabyte - MB

Megabits per second - Mbps

MIB – Management Information Base is a set of objects that can be managed by using SNMP

Modem – A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE – Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU – Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast – Sending data from one device to many devices on a network

N

NAT – Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI – NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS – Network Basic Input/Output System

Netmask – Determines what portion of an IP address designates the Network and which part designates the Host

NetWare – A Server Software developed by Novell

Network Interface Card – A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network later – The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol – Used to synchronize the time of all the computers in a network

NIC – Network Interface Card

NTP – Network Time Protocol

O

OFDM – Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI – Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF – Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password - A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network – The interconnection of networking devices within a range of 10 meters

Physical layer – The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

PoE – Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP 3 – Post Office Protocol 3 is used for receiving email

PPP – Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE – Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP – Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble – Used to synchronize communication timing between devices on a network

Q

QoS – Quality of Service

R

RADIUS – Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Rendezvous – Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater – Retransmits the signal of an Access Point in order to extend it's coverage

RIP – Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11 – The most commonly used connection method for telephones

RJ-45 - The most commonly used connection method for Ethernet

RS-232C – The interface for serial communication between computers and other related devices

RSA – Algorithm used for encryption and authentication

S

Samba – A freeware program that allows for resources to be shared on a network. Mainly used in Unix based Operating Systems

Server – A computer on a network that provides services and resources to other computers on the network

Session key – An encryption and decryption key that is generated for every communication session between two computers

Session layer – The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol – Used for sending and receiving email

Simple Network Management Protocol – Governs the management and monitoring of network devices

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SOHO – Small Office/Home Office

SPI – Stateful Packet Inspection

SSH – Secure Shell is a command line interface that allows for secure connections to remote computers

SSID – Service Set Identifier is a name for a wireless network

Stateful inspection – A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests for incoming packets are allowed to pass though the firewall

Subnet mask – Determines what portion of an IP address designates the Network and which part designates the Host

T

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TFTP – Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput – The amount of data that can be transferred in a given time period

Traceroute – A utility displays the routes between you computer and specific destination

U

UDP – User Datagram Protocol

UNC – Universal Naming Convention allows for shares on computers to be identified without having to know what storage device it's on

Unicast – Communication between a single sender and receiver

Universal Plug and Play – A standard that allows network devices to discover each other and configure themselves to be a part of the network

UPnP – Universal Plug and Play

URL – Uniform Resource Locator is a unique address for files accessible on the Internet

UTP – Unshielded Twisted Pair

V

Virtual LAN -

Virtual Private Network – A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN – Virtual LAN

Voice over IP – Sending voice information over the Internet as opposed to the PSTN

VoIP – Voice over IP

W

Wake on LAN – Allows you to power up a computer though it's Network Interface Card

WAN – Wide Area Network

Web browser – A utility that allows you to view content and interact will all of the information on the World Wide Web

WEP – Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wi-Fi – Wireless Fidelity

Wi-Fi Protected Access – An updated version of security for wireless networks that provides authentication as well as encryption

Wide Area Network - A network spanning a large geographical area or consisting of more than one LAN.

Wireless ISP – A company that provides a broadband Internet connection over a wireless connection

Wireless LAN – Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP – Wireless Internet Service Provider

WLAN – Wireless Local Area Network

Y

Yagi antenna – A directional antenna used to concentrate wireless signals on a specific location

Technical Specifications

Hardware Interface

- 4 x 10/100/1000 Auto-Sensing Gigabit Ethernet LAN Ports
- 1 x 10/100 Auto-Sensing Fast Ethernet

WAN Port

- D-Link 108G Wireless Technology

Software Features

- GameFuel™ Priority – Technology
- Up to 256 Firewall Port Configurations
- Access Control Policies (Parental Controls)
- Internal and External System Logging
- Static / Dynamic Routing
- Oversized NAT table
- Email Alerts
- Wireless Distribution System (WDS)

Dimensions

- L = 7.5 inches (190.5mm)
- W = 4.6 inches (116.84mm)
- H = 1.375 inches (35mm)

Security

- WPA-Enterprise
- WPA-Personal
- 64/128-bit WEP
- MAC Filtering

External Antenna Type

- 1 - 5dBi detachable antenna

Standards

- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3u

LEDs

- Power
- WAN
- WLAN (Wireless Connection)
- LAN

Wireless Signal Rates[1] with Automatic Fallback

- D-Link 108G: 108Mbps
- 54Mbps · 48Mbps
- 36Mbps · 24Mbps
- 18Mbps · 12Mbps
- 11Mbps · 9Mbps
- 6Mbps · 5.5Mbps
- 2Mbps · 1Mbps

Power Input

- External Power Supply DC 5V, 2.5A

Warranty

- 1-Year

[1]Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors lower actual data throughput rate.

Contacting Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link technical support through our web site, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:

(877) 453-5465

24 hours a day, seven days a week.

D-Link Technical Support over the Internet:

http://support.dlink.com

email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:

(800) 361-5265

Monday to Friday 7:30am to 12:00am EST

D-Link Technical Support over the Internet:

http://support.dlink.ca

email:support@dlink.ca

When contacting technical support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and
- Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type (“Warranty Period”), except as otherwise stated herein.

1-Year Limited Warranty for the Product(s) is defined as follows:

- Hardware (excluding power supplies and fans) One (1) Year
- Power Supplies and Fans One (1) Year
- Spare parts and spare kits Ninety (90) days

D-Link’s sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link’s sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product (“Software”) will substantially conform to D-Link’s then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days (“Warranty Period”), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link’s sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link’s functional specifications for the Software or to refund at D-Link’s sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

■ The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

■ The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

■ After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

■ The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

■ Return Merchandise Ship-To Address

USA: 17595 Mt. Herrmann, Fountain Valley, CA 92708

Canada: 2180 Winston Park Drive, Oakville, ON, L6H 5W1

(Visit http://www.dlink.ca for detailed warranty information within Canada)

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

Copyright Statement: No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

CE Mark Warning: This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

For detailed warranty outside the United States, please contact corresponding local D-Link office.

FCC Caution:

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment; such modifications could void the user's authority to operate the equipment.

(1) The devices are restricted to indoor operations within the 5.15 to 5.25GHz range. (2) For this device to operate in the 5.15 to 5.25GHz range, the devices must use integral antennas.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least eight inches (20 cm) from all persons.

This equipment must not be operated in conjunction with any other antenna.

Registration

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.